## Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

## Listing of Claims:

1. (Original)  A method for creating an authenticable image on a receiver, the method comprising the steps of:

(a)     providing a first carrier formed from information related to a physical characteristic of the receiver;

(b)     providing a second carrier that is randomly generated;

(c)     combining the first and second carrier such that the first carrier cannot be derived without the second carrier for forming a combined carrier;

(d)     combining the combined carrier with predetermined content for forming the authenticable image having the predetermined content; and

(e)     including the authenticable image having the predetermined content on the receiver.


2. (Original)  The method of claim 1, wherein step (a) includes providing fibrous content as the discernible physical characteristic of the receiver


3. (Original)  The method as in claim 2, wherein step (a) includes creating the first carrier from scanning a predetermined region of the receiver.


4. (Original)  The method of claim 1, wherein steps (a) and (b) include creating the first and second carriers by:

i)     transforming the carrier to a Frequency domain to form a transformed carrier;

ii)     shaping a spectrum of the transformed carrier to cancel the anticipated MTF effect of the print process or to facilitate the human visual system; and

iii)     inverse transforming the transformed carrier.

5. (Original) The method of claim 1 further comprising the step of encrypting the predetermined content.

6. (Original) A method of authenticating a receiver having an authenticable image that includes predetermined content integrally combined with information related to the discernible physical characteristic of the receiver, and integrally combined with a second carrier generated from a random key, the method comprising the steps of:

(a) scanning the authenticatable image on the receiver to produce information related to the discrenible physical characteristic of the receiver;

(b) discerning the physical characteristics to form the first carrier;

(c) providing a second carrier generated from a random key;

(d) discerning a message using the first and second carriers in combination with the scanned authenticable image;

(e) providing the predetermined content; and

(f) determining the authenticiy of the receiver upon comparing the message with the predetermined content.

7. (Original) The method of claim 6, wherein step (c) includes discerning the physical characteristic of the authenticated receiver by scanning a portion of the receiver on which the authenticatable image is formed.

8. (Original) The method of claim 7, wherein step (c) includes determining fibrous content as the discernible physical characteristic of the receiver.

9. (Canceled)

10. (Canceled)